McAfee Firewall Enterprise Appliance

Characterize and contain every new threat and vulnerability

Sprawling enterprise applications and the broad, fast-changing attack surface of Web 2.0 call for a new approach to firewall security. First-generation firewalls were limited to port, protocol, and IP addresses. Today, McAfee® high assurance firewalls let you confidently see and control new and existing applications for efficient, effective rules. And to detect complex threats within these applications, we integrate proactive threat intelligence with multiple inspection technologies in one cost-effective, easy-to-manage appliance.

McAfee Firewall Enterprise Features

McAfee AppPrism™ application visibility and control including:

- Packet, stateful, and full application filtering
- Full application visibility and control
- Multiple delivery options, including multi-firewall (one appliance managing up to 32 virtual firewalls), McAfee Firewall Enterprise for Crossbeam, and a virtual firewall appliance
- Network address translation (NAT)

McAfee AppPrism categories

- Anonymizers/proxies
- Authentication services
- Business web applications
- Content management
- Commercial monitoring
- Database
- Directory services
- Email
- Encrypted tunnels
- Enterprise resource planning (ERP)/ customer relationship management (CRM)
- File sharing
- Gaming
- Instant messaging
- Infrastructure services
- IT utilities
- Mobile software
- Peer-to-peer (P2P)
- Photo/video sharing
- Remote administration
- Remote desktop/terminal services
- Social networking
- Software/system updates
- Storage
- Streaming media
- Toolbars and PC utilities
- Voice over IP (VoIP)
- VPN
- Webmail
- Web browsing
- Web conferencing

Firewalls are traditionally only as strong or as weak as the policies you define. But effective security policies for today's complex Web 2.0 traffic depend on fine-grained understanding that can be hard to come by. You need rapid insight that goes far beyond port and protocol to encompass different web applications and users and the sophisticated threats that target them.

Where in the past you could await signatures, the breakneck pace of threat evolution today demands proactive, predictive diagnosis of risk. Multiple attributes, such as source reputation, content, and behavior should be assessed to reveal malicious intent before a new threat is confirmed.

It's not enough to predict the threat. Accurate, timely blocking demands concerted action that crosses conventional product silos. These demands—plus the call to prove compliance—increase the operational burden on the network team. Yet budgets remain under pressure. Something has to change.

The Biggest Firewall Innovation in 15 Years

With version 8 of the McAfee Firewall Enterprise, McAfee reinvents the firewall. Three innovations deliver unprecedented protection at an affordable price. We combine full application visibility and control, reputation-aware threat intelligence, and multivector attack protection to improve network security while shaving effort and expense.

The firewall solution includes the McAfee Firewall Enterprise appliances and McAfee Firewall Enterprise Control Center centralized management.

Today, the weakest link in network security is the application layer. We have taken our proven, high-assurance firewall—trusted by ultra-secure environments all over the world—and have added broad application discovery and control. You can now protect new and existing Web 2.0 applications from the risks of data leakage, network abuse, and malicious attacks. With McAfee technology, you can ensure the applications using your network benefit your business.

Application visibility

McAfee AppPrism technology allows you to identify all traffic and reveal the applications that are really in use, with helpful context such as source, bandwidth, and destination. By inspecting encrypted application-level traffic, you can eliminate loopholes favored by cyberthieves and attackers.

Application control

Fine-grained control allows comprehensive enforcement of policy based on business needs. Instead of policies matched just to IP address, port, or protocol, you can now place a user name with a role and a set of applications.

McAfee Firewall Enterprise Features (continued)

Authentication
- Local
- Microsoft Active Directory
- Transparent identities for Active Directory (McAfee logon collector)
- LDAP (Sun, Open LDAP, Custom LDAP)
- RADIUS
- Microsoft Windows domain authentication
- Microsoft Windows NTLM authentication
- Passport (single sign-on)
- Strong authentication (SecurID)
- Supports CAC authentication

High availability
- Active/active
- Active/passive
- Stateful session failover
- Remote IP monitoring

Global threat intelligence
- McAfee Global Threat Intelligence™ network connection reputation
- Geo-location filtering
- McAfee Labs™

Encrypted application filtering
- SSH
- SFTP
- SCP
- Bidirectional HTTPS decryption and re-encryption

Intrusion prevention system (IPS)
- More than 10,000 signatures
- Automatic signature updates
- Custom signatures
- Preconfigured signature groups

Antivirus and antispyware
- Protects against spyware, Trojans, and worms
- Heuristics
- Automatic signature updates

Web filtering
- Integrated McAfee URL filtering and management
- Block Java, Active-X, JavaScript, SOAP

Antispam
- McAfee Global Threat Intelligence network connection reputation

VPN
- IKEv1 and IKEv2
- DES, 3DES, AES-128, and AES-256 encryption
- SHA-1 and MD5 authentication
- Diffie-Hellmann groups 1, 2, and 5
- Policy-restricted tunnels
- NAT-T
- Xauth

Construct application usage rules that combine attributes such as:

- Business or recreational purpose
- User identity
- Embedded application control
- Whitelisting
- Geo-location

User identity

Without visibility into and control over users and the context of their use, firewalls cannot defend against increasingly port-agile, evasive, targeted applications. McAfee Firewall Enterprise applies user-aware rules and control over applications.

When a user connects, the system validates entitlements in real time from your existing user directory. The firewall quickly applies policies mapped to user identity that grant explicit use of an application.

By tracking to the user, rules are granular enough for modern business operation. And identity-based rules make good operational sense. More and more enterprises rely heavily on unified use of user directories and identity management to support access controls. User changes happen once and propagate out. Security policies stay up to date as the user community changes.

Embedded application control

Embedded application control gives you the power to tailor rights within an application. For instance, you might allow Yahoo!, but block Yahoo! IM, or allow IM only for specific user groups, perhaps customer support or sales or locations, such as the head office.

You can also support appropriate corporate use and blackout policies by specifying when an application can or cannot be used. Rules could allow MySpace use during lunchtime, for example, for customer service teams, while financial applications are not available to anyone via VPN on weekends.

Many exploits try to benefit from the lax security in social networking sites by concealing their payloads within trendy applets. With McAfee, you can allow access to the beneficial elements of sites like Facebook, but still minimize the risk of compromised applications within each site.

Whitelisting

For advanced control, application whitelisting lets you explicitly allow only traffic from applications that have been approved as necessary or appropriate. Compared to lengthy blacklists, whitelisting whittles down the number of rules you need to write and maintain.

Geo-location

As botnets proliferate through popular social networking applications, it has become more important to be able to lock down rogue applications that attempt to communicate to certain locations. Geo-location lets you cut off this contact to keep your data from exfiltrating and prevent your systems from being used for mischief.

We give you this fine-grained control while making rules development less complex. In fact, there's just one policy in one view. One straightforward console presents the options required to efficiently manage all rules and add defenses. This unified model is especially beneficial over time and across teams, as we also highlight rule interactions and overlaps. With colored fields highlighting potential conflicts, you avoid errors and enhance performance.

Protection

McAfee AppPrism helps you reduce risks from application-level threats while you optimize use of corporate bandwidth. Behind McAfee AppPrism stands the power of McAfee Labs™. Our threat researchers use threat research and intelligence data to continually recognize and assess risk for 31 categories of applications, ranging from anonymizers to video and photo sharing.

By assigning dynamic reputations for sites, senders, and locations, we can block an average 70 percent of undesirable traffic before you ever see it. Because of this capability, it can even spot the subtle command and control (C&C) channel of botnets.

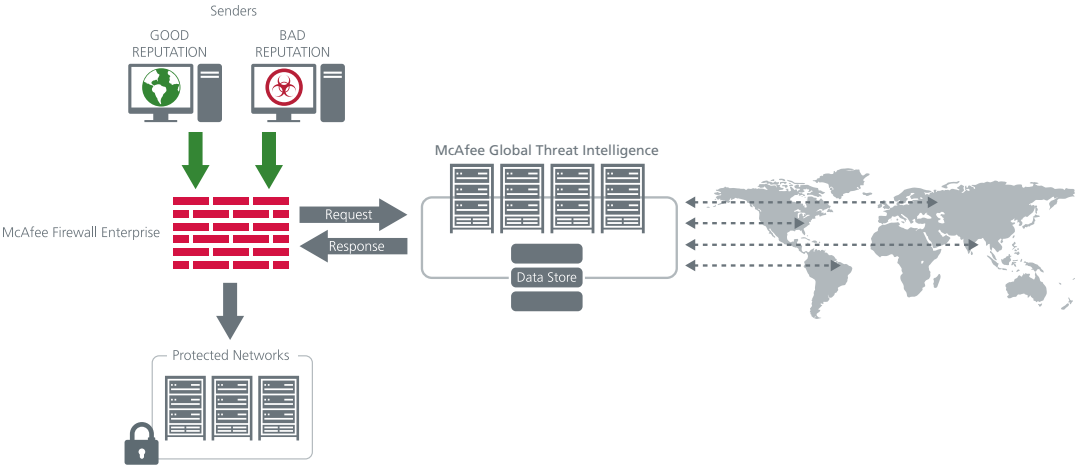

Figure 1. McAfee Global Threat Intelligence featuring McAfee TrustedSource™ allows or blocks traffic based upon reputation.

The Only Firewall with Reputation Analysis and Global Threat Intelligence

Only McAfee includes reputation technology in a firewall, and it is just one element of McAfee Global Threat Intelligence™. At McAfee, more than 400 researchers collaborate across web, spam, vulnerability, host and network intrusion, malware, and regulatory compliance research. This breadth allows them to characterize every new threat and vulnerability.

Their efforts, informed by more than 100 million sensors around the world, deliver real-time predictive risk analysis to guard you against evolving multifaceted threats.

Unlike old-fashioned firewalls that rely on signatures, automated threat feeds from McAfee Labs keep you up to date without taking your firewall off-line. With the increase in advanced persistent threats like Operation Aurora, McAfee Global Threat Intelligence is the most sophisticated protection you can own, helping you mitigate vulnerabilities, avoid regulatory violations, and lower the cost of remediation.

Multivector Security in One Integrated Appliance

One reason customers choose McAfee is our extensive security and compliance portfolio. Now, we place this might right at your door. Facing off against the complex threats in Web 2.0 applications, exploit cocktails, phishing, and targeted attacks, McAfee Firewall Enterprise now combines multiple crucial threat protections in every firewall appliance.

Before, firewalls were limited to access control and segmentation. Adequate protection required the expense of implementing and maintaining several separate products. Now, one appliance combines:

- McAfee AppPrism for full application discovery and control
- Intrusion prevention
- Global reputation analysis
- Industry-leading McAfee URL filtering
- Encrypted application filtering
- Antivirus, antispyware, and antispam

Our experience building multivector solutions has helped us deliver all these protections without compromising performance or productivity—and without adding to the cost.

McAfee SecureOS® Operating System

Features

- McAfee Type Enforcement® technology
- Preconfigured operating system (OS) security policy
- OS compartmentalization
- Network stack separation

McAfee Firewall Enterprise Control Center

- Windows graphical user interface
- Local console
- Full command line
- USB disaster recovery configuration backup and restore

Logging and monitoring

- On-box logging
- Scheduled log archiving and exporting
- McAfee Firewall Enterprise log software extract format (SEF)
- Export formats (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP v1, v2c, and v3

Networking and routing

- IPv6 compliant
- Dynamic routing (RIP v1 and v2, OSPF, BGP, and PIM-SM)
- Static routes
- 802.1Q VLAN tagging
- DHCP client
- Default route failover
- QoS

Secure servers

- Secure DNS (single or split)
- Secure sendmail (single or split)

Appliances and hardware

- Upgrade warranty to four-hour response for most models
- Virtualization solutions available
- Single-, dual-, and quad-core processors
- ASIC-based acceleration
- RAID HDD configurations
- Redundant power supplies

Technical support

- 24/7 telephone-based technical support
- 24/7 technical support with web-based ticketing and knowledgebase

McAfee Firewall Enterprise Product Line

The Firewall Enterprise product line includes appliances appropriate for businesses of all sizes, as well as companion products, such as McAfee Firewall Enterprise Control Center. Our Control Center and Firewall Enterprise appliances work together to streamline management activities and reduce operational costs. Flexible hybrid delivery options include physical appliances, multi-firewall appliances, and virtual appliances. Carrier-class security performance with speeds up to 40 Gbps is delivered by our McAfee Firewall Enterprise for Crossbeam solution running on Crossbeam's X-Series hardware. Ask your sales representative for more information.

Virtual firewall to protect your virtual infrastructure

crossbeam

Crossbeam X-Series firewall performance up to 40 Gbps

Fine-Grained Control Made Manageable

Reliable security must also be easy to configure. The intuitive McAfee Firewall Enterprise administrative console lets your administrators create rules and selectively apply defenses such as application filters, IPS signatures, and URL filtering from a single screen. New software feature updates are delivered automatically via the Internet, reducing maintenance effort. Simply determine the schedule with a single click.

The McAfee Firewall Enterprise product line includes an additional tool for simplifying management. Sold separately, McAfee Firewall Enterprise Control Center offers centralized firewall policy management for multiple McAfee Firewall Enterprise appliances. It helps you maximize operational efficiency, simplify policy control, optimize rules, streamline software updates, and demonstrate regulatory compliance. You can even compare policy configurations on all of your McAfee Firewall Enterprise Control Center-managed devices to ensure consistency across your network. Robust configuration management lets you centrally track, trace, and validate all policy changes.

Furthermore, McAfee Firewall Enterprise Control Center integrates with McAfee ePolicy Orchestrator® (McAfee ePO™) software, providing visibility into firewall health data and reports.

The Most Secure Firewall Hardware Platform

At its core, McAfee Firewall Enterprise runs on the high-speed, high-assurance McAfee SecureOS operating system. Patented McAfee Type Enforcement technology secures the OS itself for an unparalleled level of platform security. Perhaps it is why McAfee SecureOS has an unparalleled CERT advisory record: no emergency security patches have ever been required.

The preconfigured operating system security policy prevents compromises, and the entire operating system is compartmentalized so attackers cannot disrupt its work.

These extra steps allowed us to be the first firewall to achieve Common Criteria EAL 4+ certification with US DoD Protection Profile compliance.

Because of our innovation and advanced security, the McAfee Firewall Enterprise protects 15,000 networks around the world, including thousands of government agencies, Fortune 500 organizations, and seven of the top 10 financial institutions. Put McAfee to work protecting you.

Hardware Specifications[1]	S1104	S2008	S3008	S4016	S5032	S6032	S7032-XX
Form factor	Small 1U	1U	1U	Enterprise 1U	Enterprise 2U	Enterprise 2U	Enterprise 2U
Unlimited user licenses	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Recommended users	200	300	600	Medium–Large[3]	Medium–Large[3]	Large[3]	Large[3]
RAID	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Maximum network modules	N/A	N/A	N/A	1	3	3	2[4]
1 Gb copper interfaces (base/maximum)	4	8	8	8/16	8/32	8/32	8/16[4]
1 Gb fiber interface option (maximum)	N/A	N/A	N/A	8	24	24	8[4]
10 Gb fiber interface option (maximum)	N/A	N/A	N/A	6	18	18	4[4]
Encrypted filtering acceleration	N/A	N/A	Integrated	Integrated	Integrated	Integrated	N/A
Out-of-band management (status, temperature, voltage, on/off, and more)	Serial Console Only	Serial Console Only	Yes	Yes	Yes	Yes	Yes
Regulatory compliance	BSMI (Taiwan), MIC/KCC (Korea), C-Tick (Australia/NZ), VCCI (Japan), FCC (US), UL (US), CSA (Canada), ICES (Canada), CE (EU), GOST R (Russia), CCC (China), SABS (South Africa), IRAM (Argentina), NOM (Mexico)						
Performance[1]							
Firewall performance (maximum)[2]	750 Mbps	2.0 Gbps	4.0 Gbps	9.0 Gbps	12.0 Gbps	15.0 Gbps	12.0 Gbps
Threat prevention[2]	250 Mbps	1.0 Gbps	2.0 Gbps	3.0 Gbps	5.0 Gbps	6.0 Gbps	5.0 Gbps
McAfee AppPrism[2]	250 Mbps	1.0 Gbps	2.0 Gbps	7.5 Gbps	10.0 Gbps	12.0 Gbps	10.0 Gbps
Concurrent sessions[2]	200,000	500,000	750,000	1,500,000	3,000,000	4,000,000	3,000,000
New sessions per second[2]	5,000	15,000	20,000	35,000	50,000	70,000	50,000
IPSec VPN throughput (AES)[2]	60 Mbps	250 Mbps	350 Mbps	400 Mbps	450 Mbps	500 Mbps	450 Mbps
IPSec VPN maximum number of tunnels[2]	250	1,000	2,000	4,000	8,000	10,000	8,000
Dimensions, weight, environmental							
Width	16.9 in 42.93 cm	16.9 in 42.93 cm	16.9 in 42.93 cm	17.2 in 43.8 cm	18.9 in 48.04 cm	18.9 in 48.04 cm	18.9 in 48.04 cm
Depth	8.5 in 21.59 cm	28.0 in 71.12 cm	28.0 in 71.12 cm	24.4 in 61.87 cm	30.0 in 76.21 cm	30.0 in 76.21 cm	30.0 in 76.21 cm
Height	1.7 in 4.32 cm	1.7 in 4.32 cm	1.7 in 4.32 cm	1.7 in 4.32 cm	3.4 in 8.71 cm	3.4 in 8.71 cm	3.4 in 8.71 cm
Weight	10.93 lbs 4.96 kg	25 lbs 11.34 kg	25 lbs 11.34 kg	22 lbs 9.98 kg	40 lbs 18.14 kg	40 lbs 18.14 kg	40 lbs 18.14 kg
Power supply details	100 W 110/220 V	350 W 110/220 V	350 W 110/220 V	Dual 400 W 110/220 V	Dual 750 W 110/220 V	Dual 750 W 110/220 V	Dual 750 W 110/220 V
Operating temperature	10° C–35° C 50° F–95° F	10° C–35° C 50° F–95° F	10° C–35° C 50° F–95° F	10° C–35° C 50° F–95° F	10° C–35° C 50° F–95° F	10° C–35° C 50° F–95° F	10° C–35° C 50° F–95° F

1 All specification and performance results are based on the S series of appliances.
2 Version 8 performance data represents the maximum capabilities of the systems as measured under optimal testing conditions. Deployment and policy considerations may impact performance results.
3 Please contact your McAfee representative to determine proper sizing for your needs.
4 Maximum of two network modules supported (of any type), maximum of one 10 Gb network module supported (with a maximum of four transceivers populated).

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee, the McAfee logo, McAfee Labs, McAfee Global Threat Intelligence, ePolicy Orchestrator, McAfee ePO, McAfee AppPrism, McAfee Type Enforcement, and McAfee SecureOS are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied.
Copyright © 2012 McAfee, Inc.
42402ds_fwe_appliance_0312_fnl_ETMG